Kali Linux – The BackTrack Successor

On March 13, Kali, a complete rebuild of BackTrack Linux, has been released. It has been constructed on Debian and is FHS (Filesystem Hierarchy Standard) complaint. It is an advanced Penetration Testing and Security Auditing Linux distribution. It adhers completely to Debian development standards. However, one should not treat Kali Linux exactly the same as Debian.

BackTrack is an open-source Linux-based penetration testing toolset. In Backtrack, the common tools that you needed to perform a security assessment were all packaged into one nice distribution and ready to go at a moment's notice. BackTrack made it easy to create a new VM (Virtual Machine) from the downloaded ISO (International Organization for Standardization), perform the assessment, then either archive that VM (Virtual Machine) for future reference or delete it when done to remove the evidence.

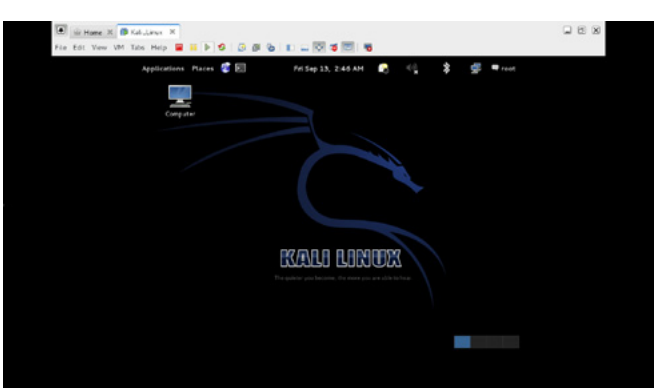

Figure 1. *Kali Linux*

Kali Linux

Kali Linux is a new open source distribution that facilitates penetration testing. Whereas BackTrack was built on Ubuntu, Kali Linux is built from scratch and constructed on Debian and is FHS (Filesystem Hierarchy Standard) compliant. Improved software repositories synchronized with the Debian repositories makes it easier to keep it updated, apply patches and add new tools. Kali Linux can also be easily customized so that it contains only the packages and features that are required. Desktop environment can also be customized to use GNOME(default), KDE (K Desktop Environment), LXDE (Lightweight X11 Desktop Environment), or whatever you prefer.

Some Other Differences

- In Kali, there is no /pentest directory like in Backtrack 5. Fire up any tool just by typing its name in the shell.
- They have removed Nessus Vulnerability Scanner in Kali, it can be manually installed by downloading it from Tenable.
- Errors like "Error connecting to wicd's D-bus bla bla" when you try to fire up Wicd in Backtrack 5 are gone. Kali Linux is much more cleaner in these respect than Backtrack 5.
- Kali Linux is Smaller in size than Backtrack 5 (which was around 3 GB approx). Kali Linux ISO is just 2 GB (approx) in size.
- Firefox has been replaced by Iceweasal. They are both given by Mozilla and very similar.

However like Firefox in Backtrack comes with 'noscript' and such add-ons for security, Iceweasal in Kali comes clean.
- Separate listing of much-hyped security tools in the Menu of Kali Linux under "Top 10 Security Tools".
- VLC Player comes pre-installed with Kali linux. In Backtrack 5, you had to manually install it and then it gave you an error saying "Won't run in root mode" and then you had to hex-edit the VLC binary.
- Light pdf viewer in Backtrack has been replaced by 'Document Viewer'.
- No 'gedit' in Kali, instead you can use 'Leafpad'.

Who Should Use Kali Linux

So, the question arises: Should I use Kali Linux? Kali Linux aims towards professional penetration testing and security auditing. To reflect these needs, several core changes have been implemented in Kali Linux:

- *Single user, root access by design*: Since it has been designed for security auditing, Kali Linux is designed to be used in a "single, root user" scenario.
- *Network services disabled by default*: Major security threats comes from various network services running on the system. Kali Linux is equipped with sysvinit hooks which disable network services by default. These hooks allow us to install various services on Kali Linux, while ensuring that our distribution remains secure by default, no matter what packages are installed. Additional services such as Bluetooth are also blacklisted by default.
- *Custom Linux Kernel*: Kali Linux uses an upstream kernel, patched for wireless injection.

Since Kali is a Linux distribution specifically geared towards professional penetration testing and security auditing and as such, it is not a recommended distribution for those unfamiliar with Linux. Misuse of security tools within your network, particularly without permission, may cause irreparable damage and result in significant consequences.

NOTE

If you are looking for a Linux distribution to learn the basics of Linux and need a good starting point, Kali Linux is not the ideal distribution for you. You may want to begin with Ubuntu or Debian instead.

Installing Kali Linux as a Virtual Machine in Virtual Box

Kali Linux can be run as Live CD or it can be installed as a virtual machine in VirtualBox. You can follow below mentioned steps to install Kali Linux as a virtual machine in VirtualBox:

- Creating a proper Virtual Machine for Kali Linux.
- Installing Kali Linux to a hard disk inside the Virtual Machine.
- Install VirtualBox Guest Addition Tools in Kali Linux.
- Setting up shared folders in VirtualBox with your Kali Linux installation.

Note

The instructions below were performed with the VirtualBox version 4.2.8. If you are experiencing issues with 4.1.x, please upgrade VirtualBox to this or a later release.

Creating the Virtual Machine

- Launch VirtualBox and using Virtual Machine Manager create a new virtual machine by clicking 'New' in the upper left corner.
- Provide a Name for the virtual machine, OS (Operating System) Type and Version. Set the Type to 'Linux' and the Version to 'Debian.' Please make sure to choose the proper version 32 or 64 bit options for your architecture. Once completed, click the continue button to move on with the setup.
- Configure the amount of memory to allocate to your new virtual machine. As a minimum allocate 2048MB. Once completed, click the Continue button.
- Next step is to create virtual machine hard drive. The default is to 'Create a virtual hard drive now.' Accept the default and click the Create button in the lower right portion of the window.
- Pick your hard drive file type. The default is VDI (VirtualBox Disk Image), however you can create any other type. For example, creating a VMDK (Virtual Machine Disk) will allow you to use this hard drive with VMWare as well as VirtualBox. Once you have selected your file type, click the Continue button.
- The next step gives you two options: to allocate the entire amount of disk space at once, OR dynamically allocate as hard drive space is needed. Once you have made your selection, click the Continue button.

- Provide hard drive file location and size. For location, it will always install in the default directory and only needs to be changed if desired.
- Approximately 8GB of disk space is required for base install of Kali Linux. It is good practice to provide roughly 4 times that amount in order to ensure proper space as you add to and update the installed system with tools and files. Once you have provided the desired size, click the Create button.

Now, the new virtual machine has been created. However, still there are few additional configuration settings that you need to make.

With your newly created Kali Linux virtual machine selected, click the 'General' link in the right portion of the Manager window. This will launch a window that allows for additional configuration settings.

At least two following changes that should be made during this step:

- Select the System option and the Processor tab to change the amount of processors. As a default, the machine is granted only 1 VCPU (Virtual CPU). Provide at least 2 processors.
- Next, select the Storage option to attach your Kali Linux ISO image. In the Storage Tree window, select your CD-ROM controller. Then within the Attributes pane click the CD-Rom Icon and 'Choose a virtual CD/DVD disk file' from the pop up menu. This will open a window to browse the host system for your Kali Linux ISO file. Once selected, click the Open button and then click the OK button to save all your changes you will be returned to the VirtualBox Manager.

You can now click the Start Button to launch the VM (Virtual Machine) and begin the Kali Linux installation process.

Kali Linux Installation to a hard disk inside virtual machine

The tutorial for installing Kali Linux can be found here. Once installation is complete, you will need to install the VirtualBox Guest Addition tools.

Install VirtualBox Guest Addition Tools in Kali Linux

In order to have proper mouse and screen integration as well as folder sharing with your host system, you will need to install the VirtualBox Guest additions.

Once you have booted into your Kali Linux virtual machine, open a terminal window and issue the following command to install the Linux Kernel headers.

```
apt-get update && apt-get install -y linux-
   headers-$(uname -r)
```

Now attach the Guest Additions CD-ROM. This can be done by selecting 'Devices' from the VirtualBox Menu and selecting 'Install Guest Additions.' It will mount the GuestAdditions ISO to the virtual CD Drive in your Kali Linux virtual machine. When prompted to autorun the CD, click the Cancel button (Figure 2).

From a terminal window, copy the VboxLinuxAdditions.run file from the Guest Additions CD-ROM to a path on your local system. Make sure it is executable and run the file to begin installation (Figure 3).

Figure 2. *Cancel_Auto_Run*

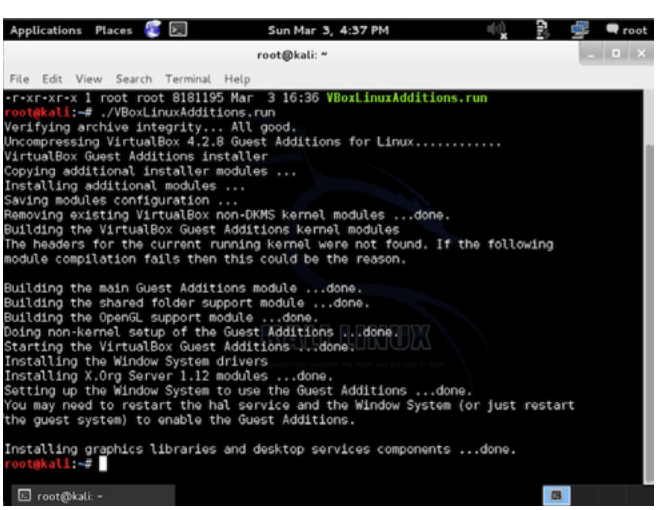

Figure 3. *VBoxAdditions_Install*

```
cp /media/cd-rom/VBoxLinuxAdditions.run /root/
chmod 755 /root/VBoxLinuxAdditions.run
cd /root
./VboxLinuxAdditions.run
```

To complete the Guest Additions installation, reboot the Kali Linux VM (Virtual Machine). Full mouse and screen integration as well as the ability to share folders with the host system should now be available.

Creating Shared Folders with the Host System

There are a few short steps that need to be completed in order to share folders on your host system with your Kali Linux VM (Virtual Machine).

From the VirtualBox Manager, select your Kali Linux VM (Virtual Machine) instance and click on the 'Shared Folders' link in the right window pane. This will launch a pop up window for adding shared folders. Within this window click the icon to add a folder.

In the Folder Path text box, provide the path to the folder you would like to share, or click the drop-down arrow to browse your host system for the path. Select the check boxes that allow for 'Auto-mount' and 'Make Permanent' and click the OK button both times when prompted (Figure 4).

Under media directory, your shared folders will now be available. A bookmark or link can also be created for easier access to the directory.

Kali Linux Forensics Mode

"Forensic Boot" introduced in BackTrack Linux that continued on through BackTrack 5 also exists in Kali Linux. The "Forensics Boot" option has proven to be very popular due to the widespread availability of our operating system. Many people have Kali ISOs laying around and when a forensic need comes up, it is quick and easy to put Kali Linux to the job. Pre-loaded with the most popular open source forensic software, Kali is a handy tool when you need to do some open source forensic work (Figure 5).

When booted into the forensic boot mode, there are a few very important changes that are made.

- The internal hard disk is not touched. This means that if swap partition exists, it will not be used and no internal disk will be auto mounted. To verify this, I removed the hard drive from a standard system. Attaching this to a commercial forensic package I took a hash of the drive. I then re-attached the drive to the computer and booted up off of Kali in forensic boot mode. After using Kali for a period of time, I then shut the system down, removed the hard drive, and took the hash again. These hashes matched, indicating that at no point was anything changed on the drive at all.

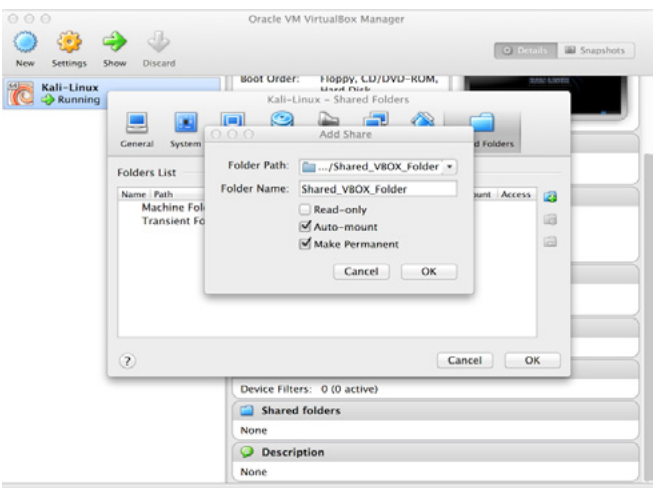

Figure 4. *Shared_Folder_Config*

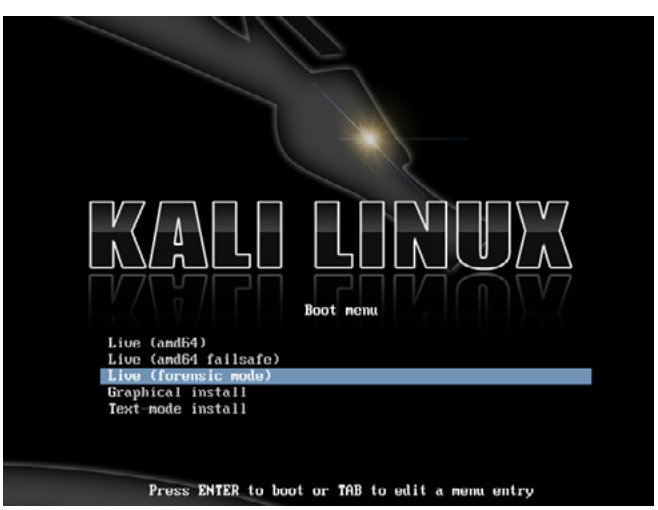

Figure 5. *Kali_Forensic_Mode*

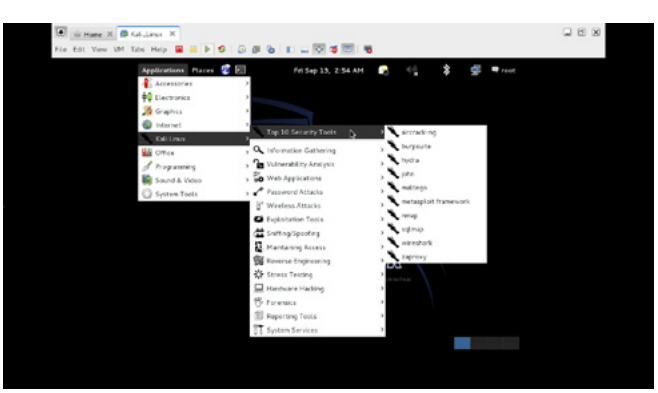

Figure 6. *Top_10_Security_Tools*

- The auto mount of any removable media has been disabled. So thumb drives, CDs, and so on will not be auto-mounted when inserted. The idea behind all of this is simple: Nothing should happen to any media without direct user action. You are responsible for doing anything as a user.

If you are interested in using Kali for real world forensics of any type, validate all forensic tools to ensure that you know their expected behavior in any circumstance that you may place them.

Exciting Tools in Kali Linux

In Kali Linux, top 10 security tools have been put under a single menu which makes life easier for most of the security enthusiast (Figure 6).

There are some other exciting tools in Kali Linux:

ACCCHECK.PL

This tool is used for Active Online Attack. It is designed as a password dictionary attack tool that targets Windows authentication via the SMB protocol. It is in fact a wrapper script around the 'smbclient' binary, and as a result is dependent on it for its execution.

Requirements

- Victim Machine: Windows XP or Windows 7 or Windows 8
- Attacker Machine: Kali Linux OS

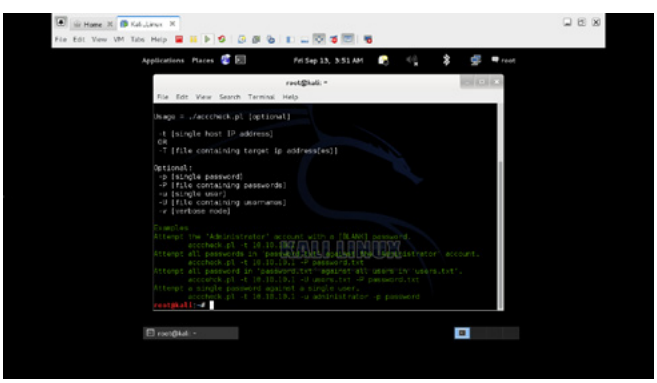

Figure 7. *acccheck_tool_cli*

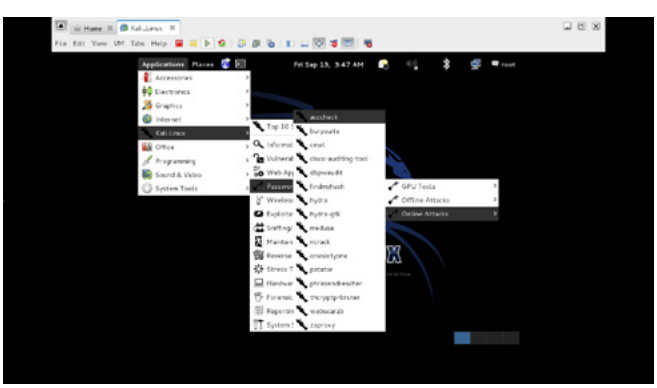

Figure 8. *acccheck_tool_GUI_Access*

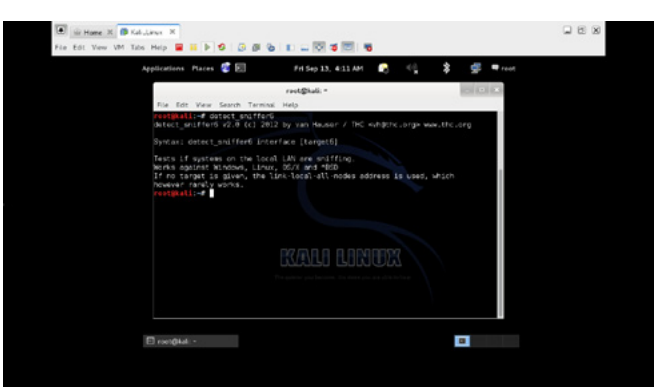

Figure 9. *detect_sniffer6_cli*

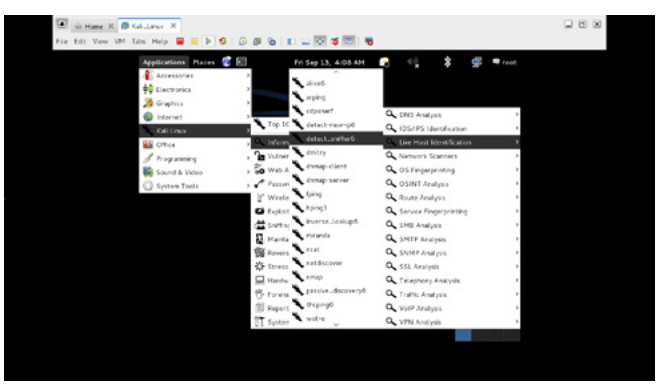

Figure 10. *detect_sniffer6_GUI_Access*

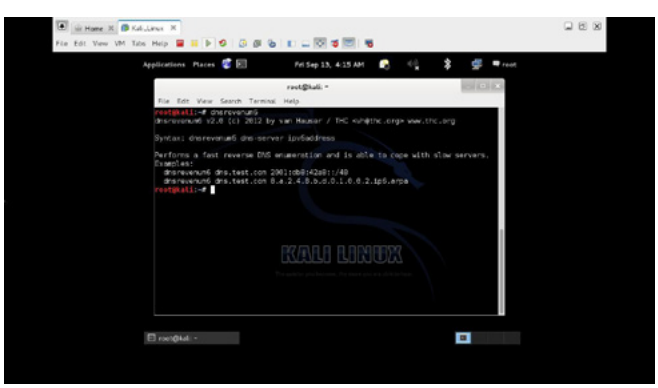

Figure 11. *dnsrevenum6_cli*

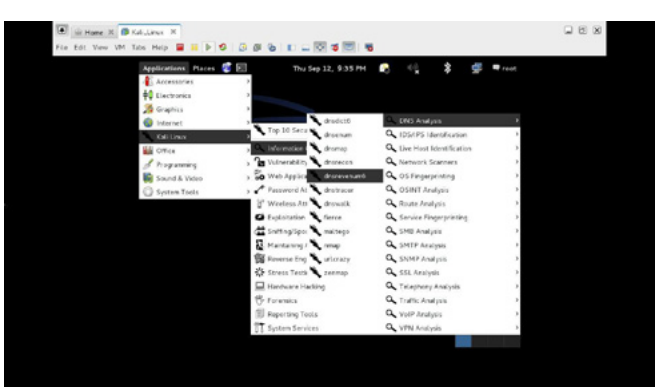

Figure 12. *dnsrevenum6_GUI_Access*

For accessing acccheck.pl tool, open terminal and type acccheck.pl and hit enter. It will display description, usage and example of the tool as shown in the Figure 7. OR, you can access this tool graphically also (Figure 8).

DETECT_SNIFFER6

This tool is used to test if systems on the local LAN are sniffing.

For accessing detect_sniffer6 tool, open terminal and type detect_sniffer6 and hit enter. It will display description, usage and example of the tool as shown in the Figure 9.

To access this tool graphically: Figure 10.

DNSREVENUM6

This tool is used for reverse DNS information gathering for IPV6.

For accessing dnsrevenum6 tool, open terminal and type “dnsrevenum6” and hit enter. It will display description, usage and example of the tool as shown in the Figure 11.

To access this tool graphically: Figure 12.

There are various other tools which can be handy as per your requirement. However, after explaining few interesting facts about Kali Linux in this article, I assume that you will be able to explore other tools on your own.

To conclude, once again I would like to emphasis that if you are really interested in professional penetration testing and security auditing, Kali Linux should be your preferred choice because most of the industry standard security tools are bundled together in this distribution.

There are other interesting information on Kali Linux. For more information, documentation is present at *http://docs.kali.org*.

SONU TIWARY

Sonu Tiwary has more than 6 years of experience in IT industry with core expertise in Linux. He is currently working as an Assistant Technical Manager with Koenig Solutions Ltd. He has vast experience on open source technologies and has also handled several projects which demand in-depth knowledge of Linux. He is an engineering graduate in Computer Science and holds Red Hat Certified Engineer (RHCE) certification.

PenTest magazine

EXTRA

Vol.3 No.5 ISSN 2084-1116
Issue 05/2013(16)

KALI LINUX 2

MAPPING WITH KALI LINUX

WI-FI TESTING WITH KALI LINUX

TESTING WEB APPS WITH KALI LINUX

BYPASSING FIREWALLS WITH KALI LINUX

TOP 10 KALI LINUX TOOLS

PLUS

INTERVIEWS WITH JEFF WEEKS AND DEMOSTENES ZEGARRA RODRIGUEZ